File reference	W17FOI290
Key words	Cybercrime
Date of release	20/06/2017
Attachments	No

Freedom of Information Act Disclosure log - Reply Extract

You asked

I am writing to you under the Freedom of Information Act 2000 to request the following information for the period 1st January 2017 to 22nd May 2017:

1. Details of any ransomware that has affected any of the IT systems used by the Plymouth Hospitals NHS Trust. In each case this should include:

    - The name of the ransomware
    - The systems affected by the attack and what it is normally used for
    - The operating system being run
    - When and for how long systems were affected
    - How the systems were affected, i.e. whether files were decrypted, systems locked, or other (please specify)
    - What would happen if the ransom was not paid
    - How the ransomware gained access to the network, i.e. phishing email, USB stick, other (please specify)
    - The ransom requested
    - If the ransom was paid and the total ransom paid for the attack
    - The number of medical activities (e.g. operations, scans, prescriptions, etc) that had to be suspended or altered during the infection period

2. Details of any other type of malware that has affected any of the IT systems used by the Plymouth Hospitals NHS Trust. In each case this should include:

    - The name of the malware
    - The systems affected by the attack and what it is normally used for
    - The operating system being run
    - How the systems were affected, i.e. whether files were decrypted, systems locked, data stolen or other (please specify)
    - When and for how long systems were affected
    - How the ransomware gained access to the network, i.e. phishing email, USB stick, other (please specify)
    - The number of medical activities (e.g. operations, scans, prescriptions, etc) that had to be suspended or altered during the infection period

3. Any correspondence between senior members of staff about incidents logged as part of 1 and 2.

4. Any correspondence between the Plymouth Hospitals NHS Trust and government departments logged as part of 1 and 2.

Our response

Beyond the information published on the Trust's website, we are not able to provide further information. Please refer to our legal statement as exemptions apply to the questions you have asked.

Our legal statement relating to the use of exemptions

Introduction

Section 31 and 38 apply to all of the questions you have asked. We are sorry that we cannot be more helpful, but trust that you will understand our approach in light of the risks associated with responding, particularly in light of recent national news events about cybercrime.

We have for some time adopted a similar approach to all requests about our integrated network security and believe this is necessary in maintaining the highest levels of security.

Exemptions applied

Section 31.-(1) (a) the prevention or detection of crime applies, as does 31.-(3) neither confirming nor denying we hold the information requested.

Section 38-(1) (a) and (b) the Health and Safety exemption applies. Additionally section 38.-(2) applies in that we are neither confirming nor denying we hold the information requested.

Exemptions use rationale

This disclosure would prejudice the prevention and detection of crime and any information, albeit confirming what we hold or do not hold could assist criminals and place our patients and staff at harm. The Trust has provided a more detailed rationale below for each exemption used and applied them following the careful consideration of submissions made to a Public Interest Test in deciding the outcome of our response to you.

Section 31 – Law enforcement- prevention of crime

We consider this exemption applies because disclosing details of our security arrangements could prejudice the security and integrity of the Trust's network and increase the risk of unauthorised access to information held by the Trust, much of which is confidential and sensitive. The level of detail that would be released would

enable external parties, who are not privy to the confidential aspects of Trust's IT systems, knowledge of our security equipment and by association its integrated network security. The Trust employs a range of security tools to mitigate the risk from different types of security threats. Firewalls, Intruder Detection Devices Antivirus and other products form a mesh of security that protects the Plymouth NHS Network and data, the more of these vectors that are known, the weaker the security of the network protection. There is a real risk that this knowledge could assist external parties in attempting a cyber-attack/hack into the Plymouth NHS Network. The anticipated harm from this is a breach of data protection (failure to protect information resulting in an unauthorised disclosure), data loss, and disruption to patient care through a loss of IT services. The severity of harm is extensive with millions of patient records put at risk of unauthorised disclosure.

Section 38 Health and Safety

Such disclosures also endanger the physical or mental health and safety of patients and staff. The dangers have become self-evident from recent events reported in the news, including delays to treatment and diagnostics to name but a few. Any failure of our infrastructure endangers both the physical and mental health of our patients and exposes them to danger.